https://www.financial-planning.com/news/finserv-firms-view-ai-tools-as-important-but-lack-proper-oversight

Finserv firms view AI tools as important but lack proper oversight
By Rob Burgess
January 08, 2025, 5:50 p.m. EST

Although many firms in the wealth management industry view artificial intelligence as important, they likely don't have proper internal oversight of its uses.

That's one takeaway from a recent survey by digital communications and archiving company Smarsh. Its "2025 Communications Compliance Survey," released last month, polled compliance and IT professionals from 262 financial services organizations — including RIAs, broker-dealers, global banks, private equity firms and insurance providers — in October.

The survey found that while 79% of firms view AI as critical to the sector's future and 81% of large firms feel pressured to adopt AI to stay competitive, only 32% have formal AI governance programs in place.

Experts say that wealth management firms should implement strategies to govern their use of AI. Having a level of human control over what is fed into these AI tools and what comes out the other end is critical to successfully implementing them into tech stacks.

How will the data be used?
Era Jain, CEO and co-founder of Zeplyn, an AI assistant for financial advisors, said RIAs are spending more time and effort on vetting their vendor processes for AI tools. RIA firms need to understand vendors' data security measures, including how data is being retained, used in training and anonymized.

"Based on our conversations, we're also finding that RIA firms are working towards instituting clear AI usage policies and offering training sessions to educate staff on both the potential of AI and the risks of misuse," she said.

Noah Damsky, principal at Marina Wealth Advisors in Los Angeles, said it is critical his firm has rules as to how they can use AI.

"We only use AI when we understand how our data will be used," he said. "If our data won't be used to train the AI model and it will stay contained, then it passes the first test."

However, Damsky said that since many other tools such as OpenAI may use the data to train the model, his firm avoids inputting any personally identifiable information (PII) or other sensitive information.

"At that point, it's like putting it on your website for everyone to see," he said.

"Have processes to determine what sort of checks need to be verified before implementing in the broader organization, especially when sensitive information is used. This is going to be an ongoing process since the space is evolving so rapidly. What works today might be prehistoric by next week, so we have to stay on our toes."

Prevent the use of unauthorized 'shadow AI' by employees

Jain said she has spoken to people at firms where advisors started harnessing ChatGPT without firm-level approval — a practice often referred to as "shadow AI." Realizing the risks, she said these firms have been educating advisors about the dangers of unsanctioned AI use, providing more guidance on approved tools and offering approved alternatives — vetted tools that meet advisors' needs. She said they also started encouraging advisors, especially those who are more tech savvy, to suggest tools they find useful, allowing IT and compliance teams to assess and onboard appropriate solutions.

"Advisors were seeing immediate efficiency gains for tasks such as drafting emails and summarizing meetings by feeding in Zoom meeting transcripts into ChatGPT, without necessarily knowing the risks of feeding in sensitive client PII to ChatGPT, as there wasn't enough awareness on how this data is getting utilized," she said. "This experience, however, exposed the strong need for advisors to adopt AI in their day-to-day workflows, and led RIA firms to take proactive steps to mitigate risks."

Alex Li, founder of AI-based education company StudyX, said that he hasn't seen the phenomenon of "shadow AI" so far at his firm. But if that behavior cropped up, employees would be asked to stop using those tools immediately and do a thorough investigation to make sure there's no data breach or other security risk.

"We will find out why employees used those unauthorized tools," he said. "Based on the findings we will consider configuring the existing tools or adjusting the approval process so employees can access the required tools and resources within a compliant framework. And to prevent such situations we will do training on AI usage norms and compliance."

Taking a different approach, Kelwin Fernandes, co-founder and CEO of AI consulting company NILG.AI, said his firm is actually promoting proactive AI usage by employees, "given well-defined guidelines about data privacy and accountability."

Review AI output accuracy and privacy, and start with clean data

Fernandes said during preliminary stages of vetting AI tools, his firm embraces AI with a human-in-the-loop on any customer-facing or critical task.

"Beyond the obvious data privacy concerns, my top concern is accountability and liability," he said. "Namely, who is responsible for a mistake made by an AI? How can I ensure we keep ownership of the outcomes, having fallback plans that

bulletproof them in case of mistakes?"

Jain said when firms consider implementing AI tools, advisors typically express concerns about exposing sensitive client information in breaches or unauthorized access, and about mistakes in AI outputs that could erode client trust, among other issues.

"While being AI-native, Zeplyn still follows a human-in-the-loop approach, and gives full control to advisors to edit any AI outputs generated in Zeplyn," she said.

Li said that while AI is good at providing answers, "We know it's not perfect."

"After AI generates answers we will do regular quality assessments and invite users to evaluate the answers," he said. "StudyX users can mark if the answers are helpful or unhelpful and provide the reason for helpful or unhelpful. We will adjust and optimize based on that. We have also introduced a manual review mechanism, and our reviewers will check the AI answers to make sure they're correct."

Tim Cooley, president, CEO and founder of DynamX Consulting in Larkspur, Colorado, has significant experience in AI using machine learning and neural networks for pattern recognition and classification. He said virtually all AI tools his firm uses are trained using scrubbed and verified data sets that are representative of the data space they are analyzing.

"Data is often collected internally, ensuring confidence in its source and collection methods," he said. "Any outputs from tools like ChatGPT are reviewed and edited to ensure accuracy, tone and intent. Additionally, project results and methods are screened and monitored by management to ensure all analyses can be explained and verified."

Said Israilov, a financial planner and wealth manager at Israilov Financial in San Francisco, said he uses AI-based notetaker Jump to summarize most of his client meetings. He said even though it does a great job of capturing discussion notes and summarizing them into actionable bullet points, his firm still thoroughly reviews these outputs to ensure their accuracy.

"We are aware that some large language models might hallucinate — generate false or misleading output," he said. "While these AI hallucinations happen in very rare cases, financial advisors who leverage AI notetakers should still closely examine their output."